National Infrastructure Protection Plan

Information Technology Sector

Homeland Security Presidential Directive 7 (HSPD-7) identified 17 critical infrastructure and key resources (CI/KR) sectors and designated Federal Government Sector-Specific Agencies (SSAs) for each of the sectors. Each sector is responsible for developing and submitting Sector-Specific Plans (SSPs) and sector-level performance feedback to the Department of Homeland Security (DHS) to enable national cross-sector CI/KR protection program gap assessments. SSAs are responsible for collaborating with public and private sector security partners and encouraging the development of appropriate information-sharing and analysis mechanisms within the sector.

Sector Overview

> *Cyberspace is the nervous system of the Nation's critical infrastructures, the control system of our country and the global economy. Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber-optic cables all powered by network, application, and security software. Collectively, these elements provide the vital flow of information that drives our critical infrastructures. Thus, the healthy functioning of cyberspace is essential to our economy and our national security.*[1]

The Information Technology (IT) Sector has a key role in securing the Nation's cyberspace. The IT Sector is composed of entities—owners and operators and their respective associations—who produce and provide hardware, software, and IT systems and services, including development, integration, operations, communications, and security.

The IT Sector is comprised of, but not limited to, the following: Domain Name System root and Generic Top-Level Domain operators; Internet Service Providers; Internet backbone providers; Internet portal and e-mail providers; networking hardware companies; and other hardware manufacturers, software companies, security services vendors, communications companies that characterize themselves as having an IT role, edge and core service providers, and IT systems integrators[2]. In addition, Federal, State, and local governments participate in the IT Sector as providers of government IT services that are designed to meet the needs of citizens, businesses, and employees.

[1] *National Strategy to Secure Cyberspace, Executive Summary*.

[2] Operating Charter of the Information Technology Sector Coordinating Council, January 24, 2006, https://www.it-isac.org/documents/itscc/index.php.

The Internet, a key component of the IT Sector, encompasses packet-based networks and databases that use a common set of protocols to communicate through various transports. The availability of the network and its services is the collective responsibility of the IT and Telecommunications sectors. Recognizing that there is a technological and industry trend toward convergence and because of the interdependent nature of IT and telecommunications, IT Sector efforts are being closely coordinated with the activities of the Telecommunications Sector.

Sector Partnerships

DHS recognizes that public-private partnerships provide the foundation for securing the IT Sector's infrastructure. The sector partnership model, as outlined in the NIPP, encourages collaboration through the respective private sector and government coordinating councils to coordinate CI/KR protection activities.

Formally chartered in January 2006, the IT Sector Coordinating Council (SCC) is composed of private companies and associations from across the sector, as well as the IT Information Sharing and Analysis Center (IT-ISAC). The IT SCC is self-organized, self-run, and self-governed. It enables owners and operators to coordinate on a wide range of sector-specific strategies, policies, activities, and issues across the public and private sector.

Chaired by DHS and established in April 2005, the IT Government Coordinating Council (GCC) includes representatives from: the Departments of Commerce, Defense, Homeland Security, Justice, State, and Treasury; the National Institute of Standards and Technology; the Office of the Director of National Intelligence; and the Office of Management and Budget. In addition, representatives from State and local governments, including the National Association of State Chief Information Officers and the Metropolitan Information Exchange, participate in the IT GCC.

CI/KR Protection Issues

The IT Sector is a key enabler for U.S. and global economies, and its products and services are relied on by all critical infrastructure sectors. Because of this reliance, IT Sector public and private security partners are actively engaged to ensure the resiliency of the sector and prevent and protect against incidents that could have negative economic consequences or degrade public confidence.

Priority Programs

A number of programs contribute to securing cyberspace and support efforts to ensure a resilient and available IT infrastructure. Included among these are:

- **United States Computer Emergency Readiness Team (US-CERT):** Established in 2003 to protect the Nation's Internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the Nation. US-CERT is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities.
- **IT-ISAC:** For operations, analysis, and information sharing, the IT-ISAC is recognized and endorsed by the IT SCC as the lead for the IT private industry. The IT-ISAC has served since 2001 and will continue to serve as a vehicle for communicating information about threats, vulnerabilities and incidents to private industry within the IT Sector.
- **InfraGard:** A partnership between the FBI and businesses, academic institutions, State and local law enforcement agencies, and other participants, InfraGard promotes the sharing of information and intelligence related to the protection of U.S. CI/KR from both physical and cyber threats. InfraGard Chapters are geographically linked with FBI Field Offices.

DHS, other Federal departments and agencies, State and local governments, academia, and the private sector manage a number of protective programs that support IT Sector situational awareness, risk management, and response, recovery, and reconstitution goals. The IT SSP will provide greater detail about these key protective programs, as well as identify gaps where additional protective programs are needed to fully meet IT Sector goals.

Homeland Security

For questions or more information, please contact NIPP@dhs.gov or visit www.dhs.gov/nipp.